ABSTRACT OF THE DISCLOSURE

A number of client systems receive a common secure transfer key pair from a server during initialization. The secure transfer private key is encrypted in the server with a platform public key sent to the server from the client system. Each client system is then able to encrypt data, using a secure transfer public key, to be recorded on a computer readable medium, and subsequently to decrypt such data using a secure transfer private key. Preferably, each client system includes an embedded security subsystem (ESS) performing cryptographic processes and providing secure key storage. Then, the secure transfer private key is stored as encrypted, and is decrypted using a private key within the ESS. Preferably, the platform private key is also stored encrypted, to be decrypted within the ESS using a hardware private key.